UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/871,525	05/31/2001	David Makower	190309-1200	1053

7590 11/02/2004

Steven M. Haas
Fay, Sharpe, Fagan, Minnich & McKee, LLP
1100 Superior Avenue,
Seventh Floor
Cleveland, OH 44114

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 11/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/871,525	MAKOWER ET AL.	
	Examiner	Art Unit	
	Brandon Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 May 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities:

- On page 5, line 4, "FIGS. 2-5" should be –FIGS. 2-6–.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. Claim 8 recites the limitation "the step of creating a client session" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-37 and 41-44 are rejected under 35 U.S.C. 102(e) as being anticipated by Wood et al. (U.S. Patent No. 6,668,322).

Regarding claim 1, Wood et al. teaches a method for transparent sign-on in a client-server environment, the method comprising the steps of:

- Receiving an encrypted communication on an originating server from a client, the client using a browser (col. 7, lines 22-25);
- Creating a challenge at the originating server (col. 7, lines 1-18);
- Sending an encrypted communication to a central sign-on server from the originating server (col. 11, lines 35-40);
- Receiving an encrypted communication on the originating server from the central sign-on server, wherein the communication received on the originating server includes a response to the communication sent to the central sign-on server (col. 11, line 43 through col. 12, line 20);
- Updating a client session on the originating server (col. 14, lines 54-59); and
- Sending another encrypted communication to the central sign-on server from the originating server (col. 14, line 60 through col. 15, line 4).

Regarding claim 2, Wood et al. teaches wherein the step of creating a challenge further comprises the step of recording on the originating server a URL requested by the

client browser, a time at which the challenge was generated, and a federation identification (col. 7, lines 9-18).

Regarding claim 3, Wood et al. teaches wherein the step of sending an encrypted communication to a central sign-on server further comprises the steps of redirecting the client browser to the central sign-on server and sending to the central sign-on server the federation identification, the challenge, and a server identification (col. 12, lines 21-24).

Regarding claim 4, Wood et al. teaches wherein the step of receiving an encrypted communication on the originating server from the central sign-on server further comprises the step of receiving a digital signature of the central sign-on server for all information communicated from the central sign-on server (col. 14, lines 54-59).

Regarding claim 5, Wood et al. teaches wherein the step of receiving an encrypted communication on the originating server from the central sign-on server further comprises the step of receiving a redirection of the client browser on the originating server (col. 12, lines 27-37).

Regarding claim 6, Wood et al. teaches wherein the step of receiving a redirection of the client browser further comprises the steps of receiving a parameter indicating that no session was present on the central sign-on server, the challenge, and

the digital signature on all of the information communicated from the central sign-on server (col. 10, lines 30-47).

Regarding claim 7, Wood et al. teaches wherein the step of receiving a redirection of the client browser further comprises the steps of receiving a parameter indicating that a session was present on the central sign-on server, the challenge, and the digital signature on all of the information communicated from the central sign-on server (col. 10, lines 30-47).

Regarding claim 8, Wood et al. teaches wherein the step of creating a client session on the originating server further comprises receiving authenticating information from the client browser (col. 13, lines 60-67).

Regarding claim 9, Wood et al. teaches wherein the step of updating a client session on the originating server further comprises creating a client session on the originating server (col. 14, lines 34-54).

Regarding claim 10, Wood et al. teaches wherein the step of sending another encrypted communication to the central sign-on server from the originating server further comprises the step of creating a digital signature on all information sent to the central sign-on server (col. 14, lines 60-64).

Regarding claim 11, Wood et al. teaches wherein the step of sending another encrypted communication to the central sign-on server further comprises the step of sending the challenge, a session time-out value, a parameter specifying that a session has been created on the originating server, a log-in identification of the client for which the session has been created, and the digital signature (col. 14, lines 60-64 and fig. 4, ref. num 420).

Regarding claim 12, Wood et al. teaches a method for transparent sign-on in a client-server environment, the method comprising the steps of:

- Receiving an encrypted communication on a central sign-on server, wherein the communication is from a web server (col. 11, lines 35-40);
- Recognizing a client on the central sign-on server (col. 11, lines 25-34);
- Sending an encrypted communication to the web server from the central sign-on server (col. 11, line 43 through col. 12, line 20); and
- Receiving another encrypted communication on the central sign-on server from the web server (col. 14, line 60 through col. 15, line 4).

Regarding claim 13, Wood et al. teaches wherein the step of receiving an encrypted communication on the central sign-on server from the web server comprises the steps of receiving a redirection of the client browser on the central sign-on server and receiving a federation identification, a challenge, an identification of the web server, and a digital signature of the web server (col. 12, line 21-24).

Regarding claim 14, Wood et al. teaches wherein the step of recognizing the client on the central sign-on server further comprises the steps of creating a cookie on the client browser and creating a record of the client on the central sign-on server (col. 11, lines 25-34).

Regarding claim 15, Wood et al. teaches wherein the step of creating a record of the client on the central sign-on server further comprises the step of using the cookie and the identification of the originating server as a concatenated primary key (col. 11, lines 35-41).

Regarding claim 16, Wood et al. teaches wherein the step of recognizing the client on the central sign-on server comprises the steps of accessing a cookie on the client browser and looking up the client on the central sign-in server based on the cookie (col. 11, lines 25-34).

Regarding claim 17, Wood et al. teaches wherein the step of looking up the client based on the cookie comprises looking up the challenge associated with the client session from a record on the central sign-on server (col. 14, lines 6-13).

Regarding claim 18, Wood et al. teaches wherein the step of sending an encrypted communication to the web server from the central sign-on server comprises

the step of creating a digital signature for all information communicated to the web server (col. 14, lines 54-59).

Regarding claim 19, Wood et al. teaches wherein the step of sending an encrypted communication to the web server from the central sign-on server further comprises the steps of redirecting the client browser back to the web server and communicating the client log-in identification for the current client session, the challenge, and the digital signature (col. 12, lines 27-37).

Regarding claim 20, Wood et al. teaches wherein the step of sending an encrypted communication to the web server from the central sign-on server further comprises the steps of redirecting the client browser back to the web server and communicating a parameter indicating that no session was present on the central sign-on server, the challenge, and the digital signature (col. 10, lines 30-47).

Regarding claim 21, Wood et al. teaches wherein the step of receiving another encrypted communication on the central sign-on server further comprises the steps of receiving an identification of the web server, a challenge, a session time-out value, and a digital signature for all information sent to the central sign-on server (col. 14, lines 60-64).

Regarding claim 22, Wood et al. teaches wherein the step of receiving another encrypted communication on the central sign-on server further comprises receiving a parameter specifying that a session has been created on the web server and a log-in identification of the client for which the session has been created (col. 14, lines 60-64 and fig. 4, ref. num 420).

Regarding claim 23, Wood et al. teaches further comprising the step of updating a record of the client session on the central sign-on server (col. 14, lines 54-59).

Regarding claim 24, Wood et al. teaches wherein the step of updating a record of the client session on the central sign-on server comprises the step of verifying a digital signature of the web server (col. 13, lines 60-67).

Regarding claim 25, Wood et al. teaches wherein the step of updating a record of the client session on a central sign-on server further comprises the steps of creating a record on the central sign-on server of the client session and the session time-out value (col. 14, lines 34-54).

Regarding claim 26, Wood et al. teaches a method for session maintenance in a transparent sign-on client-server environment, the method comprising the steps of:

- Running a session freshening task for sessions on a web server (col. 15, line 47 through col. 16, line 15);

- Sending an encrypted communication to a central sign-on server from the web server (col. 11, lines 35-40); and
- Recognizing a session on the central sign-on server (col. 11, lines 25-34).

Regarding claim 27, Wood et al. teaches wherein the step of running a session freshening task comprises the steps of looking up a list of active sessions on the web server and determining whether a session will expire on the central sign-on server before the next time the session freshening task runs (col. 16, lines 2-15).

Regarding claim 28, Wood et al. teaches wherein the step of sending an encrypted communication to the central sign-on server from the web server comprises the step of sending a server identification of the web server, the challenge used in creating the session, a new time-out value for the session, and a digital signature for all information sent in the message (col. 14, lines 60-64).

Regarding claim 29, Wood et al. teaches wherein the step of recognizing a session on the central sign-on server comprises the steps of verifying the digital signature and using the challenge to look up a record of the sessions on the central sign-on server (col. 11, lines 25-34).

Regarding claim 30, Wood et al. teaches further comprising the step of updating a client session record associated with the session on the central sign-on server (col. 14, lines 54-59).

Regarding claim 31, Wood et al. teaches wherein the step of updating a client session record comprises the step of updating a time-out value for the session on the central sign-on server (col. 16, lines 2-15).

Regarding claim 32, Wood et al. teaches a method for session maintenance in a transparent sign-on client server environment, the method comprising the steps of:

- Recognizing a client on a web server (col. 7, lines 22-25);
- Terminating a client session on the web server (fig. 2, ref. num 212);
- Sending an encrypted message to a central sign-on server (col. 11, lines 35-40);
- Recognizing the client on the central sign-on server (col. 11, lines 25-34);
- Updating a record of a session associated with the client (col. 14, lines 54-59);
- Sending an encrypted communication to a second web server, the second web server having a current local session associated with the client (col. 11, line 43 through col. 12, line 20); and
- Terminating a local session associated with the client at the second web server (fig. 2, ref. num 212).

Regarding claim 33, Wood et al. teaches wherein the step of recognizing the client on the web server comprises the step of looking up a challenge associated with a client session (col. 14, lines 6-16).

Regarding claim 34, Wood et al. teaches wherein the step of recognizing the client on the web server comprises receiving a communication from the client (col. 7, lines 22-25).

Regarding claim 35, Wood et al. teaches wherein a digital signature is created for all information communicated to the central sign-on server (col. 14, lines 60-64).

Regarding claim 36, Wood et al. teaches wherein the step of recognizing the client on the central sign-on server comprises the steps of verifying the digital signature of the web server and using the challenge to look up a record of any current session associated with the client (col. 14, lines 6-13).

Regarding claim 37, Wood et al. teaches wherein the step of updating a record of a session associated with the client comprises deleting a record on the central sign-on server (col. 6, lines 23-43).

Regarding claim 41, Wood et al. teaches a system for secure single sign-on in a client-server environment, the system comprising:

- A server, the server configured to communicate with a client (fig. 1, ref. num 110);
- A central sign-on server, the central sign-on server configured to communicate with the client and the server (fig. 1, ref. num 120 and 140); and
- Means for identifying the client on the central sign-on server (col. 11, lines 25-34).

Regarding claim 42, Wood et al. teaches wherein the means for identifying the client on the central sign-on server comprises a Single Sign-on Support URL located on the server (col. 12, lines 27-37).

Regarding claim 43, Wood et al. teaches wherein the Single Sign-on Support URL comprises means for creating a challenge when the client initiates communication with the server, means for redirecting the client browser to the central sign-on server, means for communicating the challenge to the central sign-on server, and means for receiving a communication from the central sign-on server (col. 7, lines 1-18 and col. 12, lines 21-24 and col. 11, lines 35-40 and col. 11, line 43 through col. 12, line 20).

Regarding claim 44, Wood et al. teaches wherein the server and the central sign-on server are co-located on the same server (col. 21, lines 31-42).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 38-40 and 45-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood et al. (USPN '322) in view of McCanne (U.S. Patent No. 6,785,704).

Regarding claim 38, Wood et al. teaches all the limitations of claim 32, above. However, Wood et al. does not teach wherein the step of sending an encrypted message to a second web server further comprises sending the encrypted message to each web server for which the central sign-on server has a record of an active session associated with the client.

McCanne teaches wherein the step of sending an encrypted message to a second web server further comprises sending the encrypted message to each web server for which the central sign-on server has a record of an active session associated with the client (fig. 6, ref. num 54).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine sending the message to each web server for which the

central sign-on server has a record of, as taught by McCanne, with the method of Wood et al. It would have been obvious for such modifications because each server needs the updated session.

Regarding claim 39, the combination of Wood et al. in view of McCanne teaches wherein the step of sending an encrypted message to a second web server further comprises the step of sending a parameter indicating that the client session is terminated and a digital signature of the central sign-on server (see col. 10, lines 30-47 of Wood et al.).

Regarding claim 40, the combination of Wood et al. in view of McCanne teaches wherein the step of terminating a local session associated with the client at the second web further comprises the step of verifying the digital signature of the central sign-on server (see col. 13, lines 60-67 of Wood et al.).

Regarding claim 45, Wood et al. teaches all the limitations of claim 41, above. However, Wood et al. does not teach wherein the server is a member of a federation of servers, where each member of the federation of servers is configured with a server identification, and configured to use a similar policy with regard to session management as a second server in the federation of servers.

McCanne teaches wherein the server is a member of a federation of servers, where each member of the federation of servers is configured with a server identification, and configured to use a similar policy with regard to session management as a second server in the federation of servers (fig. 6, ref. num 54 and col. 12, lines 28-47).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the server is a member of a federation of servers, where each member has a server identification, as taught by McCanne, with the system of Wood et al. It would have been obvious for such modifications because the array of servers provides scalability; the server identification uniquely identifies the individual servers.

Regarding claim 46, the combination of Wood et al. in view of McCanne teaches wherein the server in the federation of servers is configured to send encrypted messages to the central sign-on server and receive encrypted messages from the central sign-on server (see col. 11, lines 35-40 and col. 11, line 43 through col. 12, line 20 of Wood et al.).

Regarding claim 47, the combination of Wood et al. in view of McCanne teaches wherein the central sign-on server is a central sign-on server for more than one federation of servers, each federation of servers being configured with a unique federation identification (see fig. 2, ref. num 28 of McCanne).

Regarding claim 48, the combination of Wood et al. in view of McCanne teaches wherein the central sign-on server is configured to create a digital signature that is recognized by the server in the federation of servers (see col. 14, lines 54-59 of Wood et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100